

Date **20 AUG 1987**

ROUTING AND TRANSMITTAL SLIP

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. EXA/DA	<i>[Signature]</i>	20 AUG 1987
2. ADDA	<i>[Signature]</i>	20 AUG 1987
3. DDA		21 AUG 1987
4. MS/DA	<i>[Signature]</i>	21 AUG 1987
5. DDA REG.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

PER OCA: NO ANSWER IS EXPECTED
OR REQUIRED.

D/S received a copy

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
	Phone No.

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		X (W/O Atch)		
2	DDCI		X (W/O Atch)		
3	EXDIR		X (W/O Atch)		
4	D/ICS				
5	DDI				
6	DDA		X		
7	DDO		X (W/O Atch)		
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OCA		X (Advance Copy)		
14	D/PAO				
15	D/PERS				
16	D/Ex Staff				
17	D/Security/DA		X (W/Atch)		
18					
19					
20					
21					
22					
		SUSPENSE	Date		

Remarks

Per D/OCA: no answer is expected or required.

Executive Secretary

20 Aug '87

Date

STAT

DANTE B. FASCELL, FLORIDA, CHAIRMAN

LEE H. HAMILTON, INDIANA
 GUS YATRON, PENNSYLVANIA
 STEPHEN J. SOLARZ, NEW YORK
 DON BONKER, WASHINGTON
 GERRY E. STUDDS, MASSACHUSETTS
 DAN MICA, FLORIDA
 HOWARD WOLPE, MICHIGAN
 GEO. W. CROCKETT, JR., MICHIGAN
 SAM GEJDENSON, CONNECTICUT
 MERVYN M. DYMALY, CALIFORNIA
 TOM LANTOS, CALIFORNIA
 PETER H. KOSTMAYER, PENNSYLVANIA
 ROBERT G. TORRICELLI, NEW JERSEY
 LAWRENCE J. SMITH, FLORIDA
 HOWARD L. BERMAN, CALIFORNIA
 MEL LEVINE, CALIFORNIA
 EDWARD F. FEIGHAN, OHIO
 TED WEISS, NEW YORK
 GARY L. ACKERMAN, NEW YORK
 MORRIS K. UDALL, ARIZONA
 CHESTER G. ATKINS, MASSACHUSETTS
 JAMES MCCLURE CLARKE, NORTH CAROLINA
 JAIME B. FUSTER, PUERTO RICO
 JAMES H. BILBRAY, NEVADA
 WAYNE OWENS, UTAH
 FOFO I.F. SUNIA, AMERICAN SAMOA

JOHN J. BRADY, JR.
 CHIEF OF STAFF

One Hundredth Congress

EXECUTIVE REGISTRY

87-4109X

Congress of the United States
Committee on Foreign Affairs
House of Representatives
Washington, DC 20515

WILLIAM S. BROOMFIELD, MICHIGAN
 BENJAMIN A. GILMAN, NEW YORK
 ROBERT J. LAGOMARSINO, CALIFORNIA
 M. LEACH, IOWA
 TOBY ROTH, WISCONSIN
 OLYMPIA J. SNOWE, MAINE
 HENRY J. HYDE, ILLINOIS
 GERALD B.H. SOLOMON, NEW YORK
 DOUG BEREUTER, NEBRASKA
 ROBERT K. DORNAN, CALIFORNIA
 CHRISTOPHER H. SMITH, NEW JERSEY
 CONNIE MACK, FLORIDA
 MICHAEL DEWINE, OHIO
 DAN BURTON, INDIANA
 JAN MEYERS, KANSAS
 JOHN MILLER, WASHINGTON
 DONALD E. "BUZ" LUKENS, OHIO
 BEN BLAZ, GUAM

STEVEN K. BERRY
 MINORITY CHIEF OF STAFF

August 11, 1987

The Honorable William H. Webster
 Director
 Central Intelligence Agency
 Washington, D.C. 20505

Dear Judge Webster:

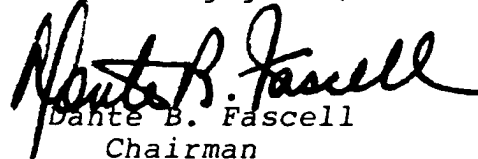
In recent months, staff members of the Committee on Foreign Affairs have met informally with representatives of your Agency in order to obtain their guidance and recommendations concerning a Standard Operating Procedure (SOP) which the committee is implementing in order to improve the protection given to classified information by the committee. The recommendations of your representatives were most helpful and have been included in the committee security SOP.

I am highly grateful for the assistance which the Agency's security experts have provided. I am especially indebted to you for the outstanding cooperation of your legislative and security staffs.

I am now enclosing a copy of the committee security SOP for your formal review and would appreciate an early reply.

With best wishes, I am

Sincerely yours,


 Dante B. Fascell
 Chairman

DBF:paj
 enclosure

CONTENTS OF STAFF OPERATING PROCEDURES FOR SECURITY:

General Comments
Handling of Classified Information
Personnel Security
Physical Security
Security for Overseas Travel

Attachments:

- A. Security Container Check Sheet
- B. Example of Safe Container Open/Close Magnetic Sign
- C. Classified Information Cover Sheet
- D. Activity Security Check List
- E. Notice of a Security Violation
- F. Record of Violation
- G. Debriefing Statement
- H. Classified Information Nondisclosure Agreement
- I. Intelligence Identities Protection Act of 1982 and Executive Order 12356
- J. Personal Security Your Personal Responsibility
- K. Security Container Information

August 6, 1987

Staff Operating Procedures for Security
for the House Foreign Affairs Committee,
U.S. House of Representatives

General: The Staff Operating Procedure (SOP) establishes uniform requirements for safeguarding classified information to which employees of the House Foreign Affairs Committee of the U.S. House of Representatives have access or possession. Each employee of the Committee is responsible for safeguarding all classified information or documents obtained and produced by the Committee. It is the responsibility of every employee of the Committee to be familiar with security requirements and to comply with them. This SOP provides guidelines concerning procedural security, physical security and personnel security matters.

Consistent with the guidance established in this document, the Top Secret Control Officer (TSCO), and or an alternate will at all times make available for immediate viewing all documents to which a requesting individual has the appropriate clearances. Determination of the need to know within each classification is the responsibility of the immediate supervisor of each employee.

If you have any questions or recommendations concerning the

PAGE 2

proper safeguarding of classified information, or any problems relating to security matters, please contact your Majority or Minority Security Officer or the Committee's Top Secret Control Officer.

Handling of Classified Information:

1. Policy: Executive Order 12356 provides a uniform system for classifying, declassifying and safeguarding national security information, a copy of which will be retained by the Committee Officer and the TSCO. Classified material originated by the Executive Branch and under the custodial control of the House Foreign Affairs Committee will be handled/safeguarded in accordance with the provisions of E.O. 12356 and this SOP. The legislative branch has derivative classification authority. Classified working papers or classified materials produced from those working papers will also be handled/safeguarded in accordance with provisions of that E.O. and this SOP.
2. Classification: The assignment of classification involves a determination of the degree of protection certain information requires in the interest of national security. There are three categories of classified information. Confidential information is information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. Secret applies to information or material the unauthorized disclosure of which could reasonably be expected to

PAGE 3

cause serious damage to the national security. Top Secret applies to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Classification of material may be supplemented by special designations and access requirements (viz., SCI Codeword, etc.)

3. Marking Classified Material: The originator of material which contains classified information is responsible for properly marking the security classification of the material. Classification designation by conspicuously marking serves to warn the holder what degree of protection is required for that information or material. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. It is essential that all classified material be marked in such a manner that it is clear to the holder what level of classification is assigned to the material. Those who originate material which contains classified information are urged to classify individual paragraphs within a document if deemed necessary. The designations "U", "C", "S", "TS", etc., shall be used at the beginning of each paragraph.

The markings shown below are required for all classified information. Since the purpose of the marking is to warn the holder that the information requires special protection, it is necessary that all classified material be marked with the appropriate markings to the fullest extent possible.

PAGE 4

a. Identification Markings: All classified material shall be marked to show the office responsible for its preparation and the date of preparation. These markings are required on the face of all classified documents.

b. Overall Markings: The overall classification of a document or any copy/reproduction thereof, shall be stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), and on the outside of the back cover (if any).

c. Page Markings: Interior pages of classified documents shall be stamped at the top and bottom with the highest classification of the information appearing thereon, or with the overall classification of the document.

d. Additional Markings: In addition to the markings specified above, classified material shall be marked, if applicable, with one or more notations which indicate the material is further restricted to special access categories.

e. Record of Classified Material - Accountability Records: The Top Secret Control Officer of HFAC shall maintain an accountability record of all classified material, to include special access materials regardless of classification. The record shall reflect as a minimum:

- date of receipt or origination (for Committee documents);

PAGE 5

classification and originator of the material; control number of the material; unclassified description of the material; disposition of the material and date thereof.

All classified materials generated by other agencies of government and other sources and officially received by the Committee will be logged in by the Top Secret Control Officer. Executive Communications and classified reports required by law will be stored in the safes of the Information System Coordinator. These materials stored in the Coordinators safes must not exceed the Secret level of classification.

6. Inventory/Accountability of Classified Material: On an annual basis, the Majority and Minority Security Officers shall conduct an inventory and accounting of all classified materials in all Committee safes. Unaccounted for documents will be turned over to the Top Secret Control Officer and materials no longer needed should be given to the Top Secret Control Officer for destruction or return to originating agency. The Top Secret Control Officer will ensure that classified documents, typewriter ribbons, and any other types of classified materials are put in a burn bag for destruction. Classified documents must be separated from typewriter ribbons and kept in separate burn bags for proper destruction.

The Top Secret Control Officer will make a list of the document titles, registry numbers if applicable and the rate of

PAGE 6

all documents delivered for destruction.

7. **Types of Classified Materials:** Classified materials include the following: Classified documents, telegrams, drafts of trip reports, letters, working papers and notes taken at closed hearings, magnetic tapes and all types of computer storage disks. All of these materials will be given the same protection as classified material which is formally identified and registered. Employees who are in doubt about the classification of an item will contact the TSCO or the originating office. Until an accurate classification is determined, the item will be given the same protection as the highest classification which may apply.

8. **Storage and Certification:** Classified material will never be left unattended. It must be secured in an approved storage container or under direct surveillance of a Committee employee with the appropriate clearance and the need to know at all times. Classified material, when not in actual use, shall be stored as follows:

a. Top Secret and Special Access materials will be stored in a General Services Administration (GSA) approved security filing cabinet (safe) bearing a GSA Test certification label. The committee safe containing these materials will be locked whenever the Top Secret Control Officer or alternate is not physically present in the room in which the safe holding these materials is located. Sensitive materials will not be removed from the room

PAGE 7

in which the Top Secret Control Officer is located, but will be read in the immediate presence of the Top Secret Control Officer or alternate. The Alternate Top Secret Control Officer, the Senior Executive Assistant, will have the same level of clearance as the Top Secret Control Officer. Under no circumstances will any Top Secret or Special Access document be removed from the room and taken to individual offices. Special Access materials will be returned by "cleared" courier to the originating agency each day.

b. Secret and Confidential Cabinets: Secret and Confidential material may be stored in a Top Secret safe or in a steel file cabinet secured by a steel bar and the three-position changeable combination padlock. Secret Orcon or Confidential Orcon materials from the CIA will not be retained overnight. Committee employees needing to review those materials will contact the Top Secret Control Officer who will arrange for courier pickup.

c. Supervision of Storage Containers: Only a minimum number of authorized persons shall possess the combinations to the storage containers of the Committee. Combinations to safes will be changed by an authorized representatives of the Clerk of the House once per year or when any individual in possession of the combination leaves the employ of the Committee. Each safe shall have a safe check sheet indicating who opens and closes each safe and the date/time thereof. See attachment A.

PAGE 8

d. Magnetic "open-closed" signs will be displayed prominently on all safes and will indicate the status of the safe. The use of these signs is an effective way to reduce security violations and serve as a prominent reminder of the status of the security container. See attachment B.

e. Any person finding a container in the open position after duty hours, will secure the container, and immediately notify the Chief of Staff of the Committee, and the TSCO who will immediately conduct an inventory of the contents of the safe. On completion of an investigation of the incident, a report will be made to the Chief of Staff to determine appropriate action. A record shall be maintained by the Top Secret Officer of the names, home phone numbers, and addresses of persons having knowledge of the combination and the location of each committee safe. See attachment K.

9. Safeguards During Use: Classified information is provided to a properly cleared person on the basis of a need-to-know in accordance with rule 20 of the Committee on Foreign Affairs. Before divulging classified information, Committee employees shall make certain of the recipient's identify, level of clearance, and need-to-know. The Top Secret Control Officer and the Majority and Minority Security Officers will maintain a current list of Committee employees whose clearance has been properly established. Employees of other agencies in the U.S. Government will be asked to produce their identification badges

PAGE 9

to determine their identification. Clearance verification of individuals from other elements of government will be done through the concerned agency's Congressional liaison office. Classified materials, when not safeguarded as provided for above, and when in actual use by cleared personnel, shall be protected as follows:

- a. Kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security control over the material.
- b. Covered (with an approved cover sheet), turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present. See attachment C.
- c. Returned to storage containers as soon as practical after use.

Consistent with the safeguards available for the protection of all levels of classified information held by the Committee, the Minority will be given equal and timely access to classified information. To accomplish this, the Top Secret Control Officer and the Senior Executive Assistant will both maintain the combination to the Top Secret Control Officer's safe.

10. Transmission: Classified material transmitted from Committee offices to any other Congressional office, government agency, or

PAGE 10

other authorized recipients, shall be registered with the Top Secret Control Officer, and properly receipted for. An OF-112, classified material receipt shall be used (see attachment). Classified materials must be double wrapped with a return address clearly marked on the outside envelope, along with instructions regarding handling of the materials should they be found.

11. Reproduction: The reproduction of classified material should be kept to a minimum. The reproduction of confidential and secret materials will be cleared with the Top Secret Control Officer. Each reproduced copy will be identified for accounting purposes in accordance with this SOP. Confidential and Secret materials may be reproduced only if the reproductions are marked or stamped with the same classification as the original. Top Secret materials will be reproduced only with the approval of the Chief of Staff and/or the Minority Chief of Staff. Codeword materials will not be reproduced. All reproductions of classified materials will be accounted for and disposed of in accordance with this SOP.

12. Duty Officer System: The Majority and the Minority Chiefs of Staff will establish a duty officer list for each building where committee offices are located. The Duty Officer shall be responsible for checking safes at close of business to ensure that they have been properly secured and will complete the activity security list. See attachment D. Unsecured containers will be closed by the Duty Officer and Notice of a Security

PAGE 11

Violation will be completed. See attachment E. The Majority/Minority Chief of Staff, on being notified, will determine the appropriate action.

13. Penalties for Security Violations: Committee employees will be subject to disciplinary action in accordance with Committee rules depending on the nature of the security violation, and the seriousness of the compromise of sensitive materials, if applicable, and the degree of responsibility of the individual involved in the security violation.

14. Transmittal of Documents: All classified materials must be double wrapped with a return address clearly marked on the outside envelope, along with instructions regarding handling of the materials should they be found, and hand carried from the sender to the recipient. Classified materials will not be given to individuals who do not have a proper security clearance. All classified materials and classified mail from other agencies to Members and staff will be delivered to the Top Secret Control Officer of the Committee for processing.

15. Electronic Processing of Classified Information:

a. Ribbons from electric typewriters can be easily read. A classified memo typed on such ribbons can be reconstructed with little effort. As such, typewriter ribbons used for the production of classified materials must be either destroyed by

PAGE 12

placing it in an approved burnbag (see the Top Secret Control Officer) or secured in an approved safe.

b. Computers: The main computer system and any computer system used by the Majority and the Minority offices of the Committee will not be used to process any type of classified information. Word processing of classified information will be done only on TEMPEST equipped, approved systems. TEMPEST refers to electronic emanations produced by electronic equipment which can be monitored and collected by sensitive radio receivers. Hostile intelligence services use these techniques to collect classified information here in Washington classified data may not be transmitted over unsecured telephone lines (e.g. Modem).

c. Telephones: Classified information will not be discussed on open telephone lines. Foreign intelligence services monitor telephone calls coming from the Congress. Individuals will not "talk around" sensitive topics.

16. Security Procedures for Closed Hearing or Briefing: The following procedures will be adhered to in preparation for a classified closed hearing or briefing:

The appropriate committee employee will notify the Official Committee Reporter (who is under the jurisdiction of the Clerk of the House), that the Hearing or Briefing will be closed and at what level of clearance will be needed. The Office (Official

PAGE 13

Reporter) will send a reporter with the appropriate clearance to record the hearing/briefing. If a hearing/briefing is CODEWORD, the CIA will accompany the reporter to transcribe the notes and remove all ribbons and tapes and return the printed transcript to the Agency, which will be forwarded to the Committee by request on a "Read and Return" same day basis. Official Committee Reporters clearances are through DOD, DOE and CIA.

Call the Sergeant-At-Arms Office and the Capitol Hill Police and request a security "sweep" of the room which is holding the hearing/briefing. The sweep is done one hour prior to the meeting, at which time the Police will remain at the door which is closed until the meeting starts to allow only Members of Congress and those staff (Committee & Member) which have the appropriate clearances and need to know to enter the room. The Police remain at the door until the hearing or briefing is completed.

Classified transcripts are delivered to the Committee (along with the tapes and ribbons), will be processed and appropriately secured.

Personnel Security:

1. General: A security clearance represents formalization of a determination that an individual is authorized access, on a "need-to-know" basis, to a specific level of classified

PAGE 14

information. Requests for clearance on the Committee originate on the Committee itself.

2. Clearance Standards for Committee Staff:

a. who are citizens of the U.S.

b. of excellent character, discretion, trustworthiness and loyalty to the U.S.

3. Investigative Requirements: To ensure that personnel meet the criteria cited above, the following coverage will be accomplished prior to granting a security clearance.

a. Confidential and Secret: A clearance for access to Confidential and Secret information shall require:

- a National Agency Check (NAC)
- a personal interview either before or as part of the investigative process
- a credit check
- written inquiries to present and past employers
- consent for access to financial records
- consent for further inquiries as may be necessary as a result of any unresolved issues surfaced in the investigation

b. Top Secret: This clearance requires, in addition to the requirements for a Secret clearance, a comprehensive field investigation of the nominee's background.

PAGE 15

c. Special Access Approvals: Certain types of classified information require special clearances and access approval.

Clearances and special access approvals are granted on a controlled need-to-know basis. A formal letter requesting such clearance must be forwarded to the Chairman. Appropriate forms must be submitted to a Budget and Fiscal Affairs staff member who will also maintain an initial clearance list. The Top Secret Control Officer and the Security Officers will maintain a record of all Special Access Clearances granted to Committee Staff. In addition, the Top Secret Control Officer will maintain a list of all personnel on Members' staffs who have a Top Secret clearance.

4. Consultants or Contract Personnel: Consultants/contract personnel must meet security approval criteria consistent with the sensitivity of assigned duties. Dependent upon the proposed use of the individuals, specific investigative requirements will be established.

5. Denials and Terminations of Security Clearances

a. Denial of Security Clearance: If, after receipt of an investigative report, the Chief of Staff, or the Minority Chief of Staff judge that a clearance should not be granted, the matter will be referred to the Chairman/Ranking Minority Member for a decision.

PAGE 16

b. Termination of Security Clearance: The Majority Chief of Staff will terminate staff security clearances of an individual if:

- (1.) the sponsoring Member requests such termination
- (2.) the employee terminates employment with the House
- (3.) the employee has committed security violations of such severity as to warrant termination of clearances

The Majority Chief of Staff will advise the agency issuing the terminated employee's clearance that he recommends that the clearance is being revoked.

6. Debriefing Program: The Majority Chief of Staff will advise the agency issuing the terminated employee's clearance that he recommends that the clearance is being revoked. Employees leaving the employ of the Committee will complete a debriefing statement which will include the following:

- observations and recommendations regarding the security of the Committee
- suspicious approaches by foreigners either in the U.S. or overseas

See attachment G.

7. Reinvestigation and Revalidation Program:

a. Committee employees are required to formally notify the

PAGE 17

Committee if they intend to get married.

b. In order to maintain the number of Committee staff having access to compartmented information at a minimum, the Top Secret Control Officer will review the need for compartmented clearances on an annual basis.

c. Reinvestigation: Committee employees holding active clearances will be reinvestigated at least every five years. The Top Secret Control Officer will advise the committee employee that a reinvestigation is required. The Majority and Minority Security Officers will also maintain a control system and coordinate with the Top Secret Control Officer to ensure that reinvestigations of staff members are accomplished.

8. Non-disclosure Agreements: A Classified Information non-disclosure Agreement must be executed by all Committee employees who are granted security clearances. The agreement will contain provisions that prohibit the signer from divulging or releasing classified information to unauthorized individuals. See attachment H. Committee employees are also required to read and sign the Intelligence Identities Protection Act of 1982. See attachment I.

9. Security Education and Awareness: The Majority and Minority Security Officers have overall responsibility for the Committee's security education program. The Committee Security Officer will

PAGE 18

ensure that before the granting of a security clearance, Committee employees are briefed on the following:

- this Staff Operating Procedure for security
- mandatory attendance at the following security education classes: Department of Defense basic class on good security practices and security awareness; State Department defensive briefing on terrorism, personal security, and the intelligence threat when traveling overseas.
- mandatory briefings are also required by various agencies when certain clearances are given.
- mandatory attendance at rebriefings regarding Committee security procedures.
- requirement to sign a non-disclosure agreement
- requirement to report suspicious contacts with foreign nationals

10. Termination of Security Clearances: Committee employees are encouraged to direct all questions concerning security matters or any security related problems to the Committee Security Officers. Committee employees whose security clearances have been revoked, whose employment has been terminated, or who are taking extended leave for a period of 60 days or more will:

- a. surrender before departure all classified documents or materials over which the Committee has custodial control
- b. again read the espionage laws

PAGE 19

c. be reminded that the non-disclosure agreement executed upon being granted a security clearance continues to be valid and that termination of employment or clearances does not release the individual from the conditions of the non-disclosure agreement.

11. Subcommittee Security Officers: The Majority and Minority Chiefs of Staff shall designate an individual in each subcommittee as a contact point for security matters.

12. Contact Reports: All Committee employees will report all contacts with persons from criteria countries, both in the United States and overseas. These reports will contain a discussion summary and an evaluation of the discussion topics, interests expressed by the foreign national, and a conclusion and recommendations about the value of further contact. Contact report shall be passed to the Majority or Minority Security Officers who will pass them to the Federal Bureau of Investigation.

Physical Security: Good physical security on the Committee has two primary focuses: One is the protection of classified materials and the other is the protection of personal effects which employees may keep in their offices. Classified material will be stored in locked safes during the day and night. When the safe is open, a cleared employee must be in the immediate area of the open safe and must maintain physical possession of

PAGE 20

any classified documents removed from that safe. Employees must never leave the room in which a safe is located and leave the safe in the open position if classified material is stored in that open repository. Classified material must never be stored in desk drawers, closets, etc. or removed from the work area and taken home at night.

Escort Policy: Employees of the Committee who have non-Committee staff visitors visit their offices will provide escort of those visitors from the reception area of their offices to their own offices. Visitors should also be escorted when they depart from Committee offices.

Personal effect to include purses, wallets, etc., should never be left unattended given the relatively open nature of most Committee offices and work areas. Any theft of personal items should immediately be reported to the Majority or Minority Security Officer and the Capitol Hill Police. See attachment J.

Security For Overseas Travel

Briefing Foreign Travel In Criteria Countries: During foreign travel to high intelligence threat countries, Committee personnel are more accessible to foreign intelligence services. To minimize the threat to the individual or to classified information, the Minority and Majority Security Officers will ensure that new Committee employees receive a defensive security

PAGE 21

briefing at the Department of State for those planning private or official travel to intelligence threat criteria countries. A list of those criteria countries is available in a classified annex to this SOP.

Classified Materials Overseas: Codels and Staffdels often receive classified briefings and take classified notes based on those sensitive briefings. Classified notes, documents, or any other sensitive materials must be stored overnight in an American Embassy/Consulate overseas, or given to a cleared embassy officer for storage in a hotel "control room" where 24-hour control is maintained over those documents by a cleared Embassy officer, or a U.S. Marine security guard.

Should Codels or Staffdels be transported via a U.S. military aircraft, classified materials can be taken on those aircraft and stored there overnight if secure 24-hour control is maintained by cleared U.S. military personnel aboard those aircraft.

Should the respective delegations be traveling via commercial aircraft, classified materials and notes taken during each Embassy or Consulate briefing or meetings should be given to the Embassy Regional Security Officer for pouching back to the Committee via the Department of State's secure courier system.

Prior to departing from the U.S., Committee delegation heads should designate an employee who will be the Classified Control

PAGE 22

Officer and be responsible for safeguarding classified materials and coordinating the safe storage of documents during overseas travel.

Classified materials taken overseas by delegations using military aircraft must be kept to a minimum both in terms of the quantity of materials and the level of classification of those materials. In general, materials classified at the Confidential or Secret level should be the highest level of classification permitted on overseas trips. Members and Staffers are strongly discouraged from carrying classified materials on commercial aircraft. Briefing books containing classified materials will be clearly marked on both the front and back cover with the highest classification of materials maintained in those briefing books. It is recommended that the classified briefing books be maintained by the Delegation head and Ranking Member and that Staffdels limit themselves to one classified briefing book.

Classified materials carried overseas or obtained there will never be left in a hotel room. Foreign intelligence services can easily gain access to hotel rooms during the day and night and can quickly photograph classified materials. This is a practice routinely followed by hostile intelligence agencies in high intelligence threat countries.

Foreign intelligence services frequently assign participants in Codels and Staffdels to hotel rooms that have been technically

PAGE 23

modified with both audio and video systems. This surveillance is highly likely in bloc countries. It is fair to assume that anything said or done in such an altered hotel room will be recorded and available to the host government's intelligence services.

While overseas, Members and Staff employees of the Committee should address any security problems or questions to the Regional Security Officer at the nearest U.S. Embassy.

Any additions or deletions to this SOP will be approved by both the Majority and the Minority Chiefs of Staff of the Committee.